

REMARKS/ARGUMENTS

By this Preliminary Amendment, Applicants (i) respond to the Office Action dated November 28, 2003 ("the Office Action") in the parent case with respect to rejected claims 1-3, 7-8, 10-11, 17-24, 26, and 29-30, (ii) present new claims 31-41 that respectively correspond to claims 4-6, 12-16, 25, and 27-28 in the parent case that the Office Action indicated to be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims, and (iii) present new claims 42-48 to round out the scope of protection. Claims 1-8 and 10-47 are now pending in this application.

102(e) Rejections

The Office Action rejected claims 1-3, 7-8, 10-11, 17-24, 26, and 29-30 under 35 U.S.C. § 102(e) as being anticipated by Wesley, et. al., U.S. Pat. No. 6,275,859 ("Wesley"). For purposes of the record, it is noted Wesley may not be prior art. However, regardless of whether Wesley does or does not represent prior art, it is respectfully submitted that Wesley, as understood, does not teach at least the following as recited in Claim 1:

" . . . wherein the key is a *symmetric* key that the sending client uses to encrypt the *multicast event* and the receiving client uses to decrypt the *multicast event* . . ." (emphasis added)

First, Wesley does not teach the encryption or decryption of "multicast events" as that term is used in Claim 1. As used in Claim 1, the term "multicast event" refers to *content* that is being delivered from one place to another, such as feature length movie content (p. 6), amateur audio content (p. 18), interactive gaming content (p. 6), or all news pay television content (p. 12). The term "multicast event" as used in Claim 1 does not refer to the underlying network *control* signals associated with the establishment of the multicasting process itself.

In contrast, as understood, Wesley relates to a particular tree-like multicast structure in which certain "repair nodes" cache the data sent by the sending node, and then retransmit any of that data that a "child node" may have missed (col. 1, lines 22-35). To help prevent malicious nodes from disrupting this data distribution scheme, Wesley teaches an authentication scheme in which a designated central authority provides participation certificates to prospective session members (col. 2, lines 59-64). Subsequently, when the nodes engage in a *session establishment dialog* with each other (col. 3, lines 6-9) they can verify each other's right to participate in the tree-like multicasting scheme using their participation certificates. Importantly, however, there is no teaching in Wesley relating to encryption or decryption of the "multicast event" itself (e.g., the movie content, the radio song content, etc.) using key information from the participation certificates.

Second, even within the unrelated context of "participation certificates", Wesley teaches away from the use of "symmetric" encryption keys. For example, column 5, lines 21-26 state, "The use of a common group key (known as a symmetric key) for authentication in a multicast setup is generally less secure than other approaches, because the key is known to many nodes." In the detailed description, Wesley then proceeds to teach only the use of *asymmetric* encryption keys (col. 4, lines 15-20). Indeed, it is well known that digital signatures, such as those used in conjunction with Wesley's "participation certificate" scheme, can only be generated and used by asymmetric cryptosystems. In summary, it is respectfully submitted that Wesley does not teach "wherein the key is a *symmetric* key that the sending client uses to encrypt the *multicast event* and the receiving client uses to decrypt the multicast event" as recited in Claim 1.

For reasons similar to those presented above in relation to Claim 1, it is further submitted that independent claims 7, 19, and 22 are likewise not anticipated by Wesley. (Claim 7 has been amended to provide grammatical correction/antecedent basis). It is

submitted that each of the pending dependent claims depending from claims 1, 7, 19, and 22 is allowable as depending from an allowable base claim.

Claims 29 and 30 have each been amended to recite, "wherein the key is a symmetric key used by a sending client to encrypt the event and used by the receiving client to decrypt the event" and are therefore submitted to be allowable for reasons similar to those presented above for Claim 1.

New Claims 31-41

(Note: It is believed that there was a typographical error in Paragraph 4 of the Office Action, and that it was not intended to read as "Claims 4-6, 12-16, 2, and 27-26 . . ." but was instead intended to read as "Claims 4-6, 12-16, 25, and 27-28 . . .")

New claims 31-41 correspond respectively to claims 4-6, 12-16, 25, and 27-28 in the parent case, the Office Action indicating those claims to be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. Accordingly, it is submitted that new claims 31-41 are in condition for allowance.

New Claims 42-48

New claims 42-48 have been added to round out the scope of protection for the Applicants' invention. Each of the claims 42-48 is supported by the specification text and/or drawings as initially filed and no new matter has been added.

CONCLUSION


In view of the foregoing remarks, Applicants submit that this claimed invention is allowable over the references cited against this application. Applicants therefore request the entry of this Amendment, reconsideration and reexamination of the application, and the timely allowance of the pending claims.

Please grant any extensions of time required to enter this response and charge any additional required fees to our Deposit Account No. 06-0916 .

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: May 26, 2004

By: 
Andrew B. Schwaab
Reg. No. 38,611

FINNEGAN, HENDERSON, FARABOW
GARRETT & DUNNER, L.L.P.
1300 I Street, NW
Washington, D.C. 20005
(202) 408-4000